103.30 Tests for divisibility by prime numbers

We know that a number is even if, and only if, its units digit is even, and a number is a multiple of 5 if, and only if, its units digit is 0 or 5. For all primes other than 2 and 5, however, there is no simple "units digit" test for divisibility. In this short note, we give a general recursive divisibility test based upon units digits. Our aim is to find a way of going from a number with d digits (in base 10) to one with $d - 1$, while preserving divisibility.

This has been done in the following result.

Theorem: Assume that the positive integer n is given, and p is a prime number other than 2 or 5. We let u and r be the units digits of p and n, respectively. Then $p \mid n$ if, and only if, $p \mid \left[\frac{n}{10}\right] - ar$, where

$$a = \begin{cases} \dfrac{up - 1}{10} & \text{if } u = 1 \text{ or } 9 \\ \dfrac{(10 - u)p - 1}{10} & \text{if } u = 3 \text{ or } 7. \end{cases} \tag{1}$$

Furthermore, if $0 < a < p$, then a is unique.

We recall the notation $[x]$, which as usual refers to the integer part of the real number x. We note that in the theorem, the number of digits of $\left[\frac{n}{10}\right] - ar$ is one less than the number of digits of n. Thus, repeating the statement of the theorem, finally we obtain a much smaller number than n to test its divisibility by a given prime. Here is an example.

Let $p = 13$ and $n = 897$. We have $u = 3$, and thus $a = \dfrac{7p - 1}{10} = 9$. Also, $r = 7$. Thus $\left[\frac{n}{10}\right] - ar = 89 - 9 \times 7 = 26$, and clearly $13 \mid 26$. So, we conclude that $13 \mid 897$.

Proof of the Theorem: We write $n = 10q + r$ where $0 \leqslant r \leqslant 9$, and $p = 10t + u$ where $u = 1, 3, 7$ or 9. We have $q = \left[\frac{n}{10}\right]$, and we wish to find an integer x such that $p \mid n$ if, and only if, $p \mid (q + x)$. If $p \mid (q + x)$, then $p \mid (10q + 10x)$, and by using the relation $10q = n - r$, we obtain $p \mid (n - r + 10x)$. We note that $\gcd(10, p) = 1$. Thus, the congruence

$$10x \equiv r \pmod{p} \tag{2}$$

has a unique solution modulo p satisfying $p \mid (10x - r)$. Hence, we obtain $p \mid n$. Conversely, we assume that $p \mid n$ or $p \mid (10q + r)$. By using (2) we obtain $p \mid 10(q + x)$, and then, because if $p \mid ab$ and $p \nmid a$ then $p \mid b$, we get $p \mid (q + x)$.

Hence, the required x satisfies (2). To find it, we note that there exists a unique a with $0 < a < p$, such that $10a \equiv -1 \pmod{p}$ or $10(-ar) \equiv r \pmod{p}$. So, we may take $x = -ar$. To determine the exact

https://doi.org/10.1017/mag.2019.112 Published online by Cambridge University Press

value of a we use the relation $10a \equiv -1 \pmod{p}$ to write $10a + 1 = pk$ for some integer k. Considering the inequality $0 < a < p$, we obtain the validity of $\frac{1}{p} < k < 10 + \frac{1}{p}$ for any prime p other than 2 or 5. This fact, together with $k \neq 10$, implies that $0 < k < 10$. Thus we have $pk \equiv 1 \pmod{10}$ with $0 < k < 10$. Now, if $u = 1$ then the conditions $pk \equiv 1 \pmod{10}$ and $0 < k < 10$ imply that $k = 1$, and consequently $a = \frac{p-1}{10}$. A similar argument implies (1) for the other values of u.

This completes the proof.

Acknowledgement: I express my gratitude to Professor Underwood Dudley for careful reading of the manuscript and giving many valuable suggestions and corrections, which improved the presentation of the Note.

10.1017/mag.2019.112

MEHDI HASSANI

Department of Mathematics, University of Zanjan, University Blvd., 45371-38791, Zanjan, Iran

e-mail: *mehdi.hassani@znu.ac.ir*

103.31 Factorising numbers with oracles

A useful classroom game

A teacher asks the students to determine the values of two positive integers a, b from the given values of the product ab, and the sum $a + b$. The students try to factorise the product, and see if the sum of the factors is the same as that for the given sum. If we set a, b to be primes of modest size, the game becomes more of a challenge, because factorisation is no longer easy.

The aim of the exercise is, of course, the introduction of the quadratic equation. The identity $(x - a)(x - b) = x^2 - (a + b)x + ab$ reveals that the game amounts to finding the roots of the equation obtained by setting the right-hand side to be zero. There is now a good incentive for the derivation of the formula for the solutions of a quadratic equation, and the game is over with the values for a, b being given by

$$a, b = \frac{(a + b) \pm \sqrt{(a + b)^2 - 4ab}}{2}. \tag{1}$$

However, a well-informed teacher may remind the students of the salient point concerning the game:

The factors of a product can be recovered from the values of the product and the sum of the factors, without resorting to a brute force factorisation scheme.

https://doi.org/10.1017/mag.2019.112 Published online by Cambridge University Press